Risk Mitigation Checklist

Most tech is designed with the best intentions. But once a product is released and reaches scale, all bets are off. The Risk Mitigation Manual presents **eight risk zones** where we believe **hard-to-anticipate *and* unwelcome consequences are most likely to emerge.**

Different tech runs different risks.
This checklist will help you prioritize your efforts.

HOW IT WORKS:

Choose a technology, product or feature you're working on. Read through the checklist and **identify the questions** and **risk zones** most relevant to you and the technology you've chosen. **Use the "Now what?" action items** to start investigating and mitigating these risks.

Risk Zone 1: **Truth, Disinformation, and Propaganda**

- ❑ What type of data do users expect you to accurately share, measure or collect?
- ❑ How could bad actors use your tech to subvert or attack the truth? What could potentially become the equivalent of fake news, bots or deepfake videos on your platform?
- ❑ How could someone use this technology to undermine trust in established social institutions, like media, medicine, democracy, science? Could your tech be used to generate or spread misinformation to create political distrust or social unrest.
- ❑ Imagine the form such misinformation might take on your platform. Even if your tech is meant to be apolitical in nature, how could it be co-opted to destabilize a government?

Risk Zone 2: **Addiction & the Dopamine Economy**

- ❑ Does the business model behind your chosen technology benefit from maximizing user attention and engagement—i.e., the more, the better? If so, is that good for the mental, physical or social health of the people who use it? What might not be good about it?
- ❑ What does "extreme" use, addiction or unhealthy engagement with your tech look like? What does "moderate" use or healthy engagement look like?
- ❑ How could you design a system that encourages moderate use? Can you imagine a business model where moderate use is more sustainable or profitable than always seeking to increase or maximize engagement?
- ❑ If there is potential for toxic materials like conspiracy theories and propaganda to drive high levels of engagement, what steps are being taken to reduce the prevalence of that content? Is it enough?

Risk Zone 3: **Economic & Asset Inequalities**

- ❑ Who will have access to this technology and who won't? Will people or communities who don't have access to this technology suffer a setback compared to those who do? What does that setback look like? What new differences will there be between the "haves" and "have-nots" of this technology?
- ❑ What asset does your technology create, collect, or disseminate? (example: health data, gigs, a virtual currency, deep AI) Who has access to this asset? Who has the ability to monetize it? Is the asset (or profits from it) fairly shared or distributed with other parties who help create or collect it?
- ❑ Are you using machine learning and robots to create wealth, rather than human labor? If you are reducing human employment, how might that impact overall economic well-being and social stability? Are there other ways your company or product can contribute to our collective economic security, if not through employment of people?

Risk Zone 4: **Machine Ethics & Algorithmic Biases**

- ❑ Does this technology make use of deep data sets and machine learning? If so, are there gaps or historical biases in the data that might bias the technology?
- ❑ Have you seen instances of personal or individual bias enter into your product's algorithms? How could these have been prevented or mitigated?
- ❑ Is the technology reinforcing or amplifying existing bias?
- ❑ Who is responsible for developing the algorithm? Is there a lack of diversity in the people responsible for the design of the technology?
- ❑ How will you push back against a blind preference for automation (the assumption that AI-based systems and decisions are correct, and don't need to be verified or audited)?
- ❑ Are your algorithms transparent to the people impacted by them? Is there any recourse for people who feel they have been incorrectly or unfairly assessed?

Risk Zone 5: **Surveillance State**

- ❑ How might a government or military body utilize this technology to increase its capacity to surveil or otherwise infringe upon the rights of its citizens?
- ❑ What could governments do with the data you're collecting about users if they were granted access to it, or if they legally required or subpoenaed access to it?
- ❑ Who, besides government or military, might use the tools and data you're creating to increase surveillance of targeted individuals? Whom would they track, why—and do you want your tech to be used in this way?
- ❑ Are you creating data that could follow users throughout their lifetimes, affect their reputations, and impact their future opportunities? Will the data your tech is generating have long-term consequences for the freedoms and reputation of individuals?
- ❑ Whom would you not want to use your data to surveil and make decisions about individuals, and why not? What can you do to proactively protect this data from being accessible to them?

Risk Zone 6: **Data Control & Monetization**

- ❑ Do your users have the right and ability to access the data you have collected about them? How can you support users in easily and transparently knowing about themselves what you know about them?
- ❑ If you profit from the use or sale of user data, do your users share in that profit? What options would you consider for giving users the right to share profits on their own data?
- ❑ Could you build ways to give users the right to share and monetize their own data independently?
- ❑ What could bad actors do with this data if they had access to it? What is the worst thing someone could do with this data if it were stolen or leaked?
- ❑ Do you have a policy in place of what happens to customer data if your company is bought, sold or shut down?

Risk Zone 7: **Implicit Trust & User Understanding**

- ❑ Does your technology do anything your users don't know about, or would probably be surprised to find out about? If so, why are you not sharing this information explicitly—and what kind of backlash might you face if users found out?
- ❑ If users object to the idea of their actions being monetized, or data being sold to specific types of groups or organizations, though still want to use the platform, what options do they have? Is it possible to create alternative models that build trust and allows users to opt-in or opt-out of different aspects of your business model moving forward?
- ❑ Are all users treated equally? If not—and your algorithms and predictive technologies prioritize certain information or sets prices or access differently for different users—how would you handle consumer demands or government regulations that require all users be treated equally, or at least transparently unequally?

Risk Zone 8: **Hateful & Criminal Actors**

- ❑ How could someone use your technology to bully, stalk, or harass other people?
- ❑ What new kinds of ransomware, theft, financial crimes, fraud, or other illegal activity could potentially arise in or around your tech?
- ❑ Do technology makers have an ethical responsibility to make it harder for bad actors to act?
- ❑ How could organized hate groups use your technology to spread hate, recruit, or discriminate against others? What does organized hate look like on your platform or community or users?
- ❑ What are the risks of your technology being weaponized? What responsibility do you have to prevent this? How do you work to create regulations or international treaties to prevent the weaponizing of technology?

YOU'VE CHECKED YOUR RISKS. NOW WHAT?

- Use the questions you've checked to **kickstart conversations** within your company or team. How can you start to correct or mitigate these risks?
- Build the checklist into your **product design requirements**.
- Distribute your top questions to your **board and advisors** to get their input.
- **Post the questions** around your office where they can help keep these ethical issues top of mind.
- **Collect resources and seek out experts** around your top risk areas to inform your strategy and design.
- **Revisit the checklist** whenever you're starting development or planning to scale a new product or service.

Get the full Ethical OS toolkit at ethicalOS.org

INSTITUTE FOR THE FUTURE | OMIDYAR NETWORK